IN THE CLAIMS

What is claimed is:

1. (Previously Presented) A method comprising:

providing a trusted platform within a computer system for applications, the trusted platform including a protected section of memory that is inaccessible to direct memory access and an unprotected section of memory that is accessible to direct memory access;

executing an application in the trusted platform;

providing a trusted path between the application and a SIM device that includes a SIM card, the SIM device being physically connected with the computer system, the trusted path being a path through a trusted port of a chipset included in the computer system, wherein the trusted port is mapped to the protected section of memory;

providing an untrusted path between the application and the SIM device, the untrusted path being a path through an untrusted port of the chipset, wherein the untrusted port is mapped to the unprotected section of memory;

exchanging unencrypted data that includes an encryption key between the SIM device and the application via the trusted path, wherein the unencrypted data to be exchanged is secured from unauthorized access via properties of the trusted path;

encrypting additional data using the encryption key; and

exchanging the encrypted data between the SIM device and the application via the untrusted path.

2. (Canceled)

3. (Previously Presented) The method of claim 1, wherein exchanging the encryption key includes the application transmitting the encryption key to the protected section of memory within the computer system; and

the SIM device accessing the encryption key from the protected section of memory.

4. (Previously Presented) The method of claim 1, wherein exchanging the encryption key includes the application accessing the encryption key from the SIM device, the application accessing the encryption key via the trusted port of the chipset.

5. (Previously Presented) The method of claim 1, wherein exchanging the encryption key includes exchanging multiple encryption keys, and exchanging the encrypted data includes exchanging separate units of data, with each unit of data separately encrypted with an encryption key selected from the multiple encryption keys.

6. (Previously Presented) The method of claim 1, wherein exchanging the encrypted data includes a host controller transmitting data from the SIM device to the unprotected section of memory, and a driver transmitting data from the unprotected section of memory to the application.

7. (Canceled)

8. (Previously Presented) The method of claim 6, wherein the host controller is a Universal Serial Bus (USB) host controller and the driver is a USB driver.

9. (Previously Presented) The method of claim 1, wherein exchanging the encryption key includes the SIM device reading the encryption key from the protected section of memory via the trusted port of the chip set.

10. (Previously Presented) The method of claim 1 further comprising:

the application decrypting the encrypted data using the encryption key.

11. (Previously Presented) The method of claim 1 further comprising:

prior to exchanging the encryption key, the application authenticating the SIM device.

12. (Previously Presented) The method of claim 6, further comprising:

exchanging a new encryption key based on a predetermined event selected from a group comprising of, each new transaction, passage of a predetermined period of time, and exchange of a predetermined amount of data.

13. (Previously Presented) A system comprising:

a system memory having a protected section that is inaccessible to direct memory access, an unprotected section that is accessible to direct memory access and a protected memory table that identifies the protected section and the unprotected section;

a processor having a private cache memory that has protections that prevent access to said private cache memory by unauthorized devices, and registers that identify memory pages of the system memory that are accessible only to trusted code;

a chipset having a trusted port mapped to the protected section of the memory

and an unprotected port mapped to the unprotected section of the memory, the system memory, processor and chipset being components of a platform that is configured to provide a trusted environment for an application; and

a SIM device that includes a SIM card, the SIM device being physically connected with the platform, to exchange unencrypted data that includes an encryption key with an application executed in the trusted environment via the trusted port, wherein the unencrypted data to be exchanged is secured from unauthorized access by the trusted port, and to exchange encrypted data with the application via the unprotected port.

14. (Canceled)

15. (Previously Presented) The system of claim 13, wherein the exchange of the encryption key includes the application to transmit the encryption key to the protected section of memory, and the SIM device to access the encryption key from the protected section of memory.

16. (Previously Presented) The system of claim 13, wherein the exchange of the encryption key includes the application to access the encryption key from the SIM device, the application to access the encryption key via the trusted port of the chipset.

17. (Previously Presented) The system of claim 13, wherein the exchange of the encryption key includes an exchange of multiple encryption keys, and the exchange of encrypted data includes an exchange of separate units of data, with each unit of data separately encrypted with an encryption key selected from the multiple encryption keys.

18. (Previously Presented) The system of claim 13, wherein the system further includes a host controller to transmit data from the SIM device to the unprotected section of memory.

19. (Previously Presented) The system of claim 18, wherein the system further includes a driver to transmit data from the unprotected section of memory to the application.

20. (Previously Presented) The system of claim 19, wherein the host controller is a Universal Serial Bus (USB) host controller and the driver is a USB driver.

21. (Previously Presented) The system of claim 13, wherein the SIM device is to read the encryption key from the protected section of memory via the trusted port of the chip set.

22. (Previously Presented) The system of claim 13, wherein the application is to decrypt the encrypted data using the encryption key.

23. (Previously Presented) The system of claim 13, wherein the application is to authenticate the SIM device prior to the exchange of the encryption key.

24. (Previously Presented) The system of claim 13, wherein a new encryption key is to be exchanged based on a predetermined event selected from a group comprising of, each new transaction, passage of a predetermined period of time, and exchange of a predetermined amount of data.

25. (Previously Presented The method of claim 1, further comprising:

determining, by the SIM device, that the application is executed in the trusted platform before exchanging the unencrypted data.

26. (Withdrawn) A method comprising:

providing a trusted platform within a computer system for applications, the trusted platform including a protected section of memory that is inaccessible to direct memory access and an unprotected section that is accessible to direct memory access;

executing an application in the trusted platform;

providing a trusted path between the application and a SIM device that includes a SIM card, the SIM device being physically connected with the computer system, the trusted path being a path through a trusted port of a chipset included in the computer system, wherein the trusted port is mapped to the protected section of memory;

providing an untrusted path between the SIM device and the application, the untrusted path being a path through an untrusted port of the chipset, wherein the untrusted port is mapped to the unprotected section of memory; and

exchanging unencrypted data between the SIM device and the application via the trusted path, wherein the unencrypted data to be exchanged is secured from unauthorized access via properties of the trusted path.

27. (Withdrawn) The method of claim 26, further comprising:

determining, by the SIM device, that the application is executed in the trusted platform before exchanging the unencrypted data.

28. (Withdrawn) The method of claim 1, wherein the properties of the trusted path include inaccessibility from applications executed outside of the trusted platform, access to the trusted path being controlled by page table registers of a processor.